UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/055,572	10/19/2001	Tom L. Nguyen	42390P12549	6116

8791 7590 09/25/2006

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
BESROUR, SAOUSSEN	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 09/25/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/055,572	**Applicant(s)** NGUYEN ET AL.	
	Examiner Saoussen Besrour	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 April 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22 and 26-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22 and 26-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to amendment filed 4/18/2006. Claims 1, 3, 5, 6, 7, 8, 10, 11, 12, 13, 14, 17, 20, 21, 26 and 27 were amended. Claims 23-25 were cancelled. Claims 1-22 and 26-30 are pending. Applicant's arguments/ amendments with respect to new claims 1-22 and 26-30 have been fully considered but they are not persuasive. The Examiner would like to point out that this action is made final (See MPEP 706.07a).

Response to Arguments

2. Applicant's arguments with respect to claim1, 3, 5, 6, 7, 8, 10, 11, 12, 13, 14, 17, 20, 21, 26 and 27 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. **Claims 1, 4, 8, 9 and 10** are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per **claim 1**, the limitation "a processing unit coupled to the non-volatile data storage device" is indefinite because it is not clear which non-volatile storage device

Applicant is referring to. For the purpose of this examination, Examiner presumes "the non-volatile-data storage device" to be the one which holds the CMOS BIOS data.

As per **claim 4**, the limitation "the validity of the data stored in the non-volatile storage device" is indefinite because it is not clear which data Applicant is referring to. For the purpose of this examination, Examiner presumes "the data stored in the non-volatile storage device" to be the CMOS BIOS data.

As per **claim 8**, the limitation "the current data in the non-volatile storage device" is indefinite because it is not clear which data Applicant is referring to. For the purpose of this examination, Examiner presumes "the data stored in the non-volatile storage device" to be the CMOS BIOS data.

As per **claim 9**, the limitation " the current data in the non-volatile storage device" is indefinite because it is not clear which data Applicant is referring to. For the purpose of this examination, Examiner presumes "the current data in the non-volatile storage device" to be the CMOS BIOS data.

As per **claim 10**, the limitation "the current content" is indefinite because it is not clear which content Applicant is referring to. For the purpose of this examination, Examiner presumes "the data stored in the non-volatile storage device" to be the CMOS BIOS.

Claims 2, 3, 5, 6, 7 and 11-16 are also rejected because they incorporate matter of their base claim.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. **Claims 1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 15, 16, 17, 18, 19, 20, 21, 22, 26, 27 and 28** are rejected under 35 U.S.C. 103(a) as being unpatentable over Harding et al. (U.S. Patent No. 6,651,188) in view of Leavitt et al. (U.S. Patent No. 5,918,014).

As per **claim 1**, Harding et al. discloses: a non-volatile data storage device, configured as one or more storage regions to store one or more bytes of CMOS BIOS data, wherein the device lacks hardware security such that some of the CMOS BIOS regions are modifiable by an application program on the system (Column 2, Lines 67-Column 3, Line 1, may be revised) another non-volatile data storage device to store a mirror image of the CMOS BIOS data (Fig. 1, item 113); a program to store one or more processor-readable instructions to ascertain the validity of the CMOS BIOS data stored in the non-volatile storage device (Fig. 1, Item 115 (validate) Column 3, Lines 4-12); and a processing unit coupled to the non-volatile storage device and program store, to read and process the one or more instructions in the program store (Column 3, Lines 13-16).

Harding et al. does not explicitly teach: if invalid to replace the CMOS BIOS data in the non-volatile storage device with the mirror image of the data. However, Leavitt et al. discloses: if invalid to replace the CMOS BIOS data in the non-volatile storage device with the mirror image of the data (Fig.3, items 116-118). Therefore it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teachings of Leavitt et al. in conjunction with the teachings of Harding et al. for the benefit of providing alternate BIOS code blocks in case primary BIOS code blocks are invalid as taught by Leavitt et al. in Column 2, Lines 15-17.

As per **claim 10**, Harding et al. discloses: reading current CMOS BIOS content stored in a non-volatile storage device of a system, wherein the device lacks hardware security such that the CMOS BIOS content is modifiable by an application program in the system (Column 2, Lines 67-Column 3, Line 1, may be revised); reading from a valid image of the CMOS BIOS content, that is stored in a further non-volatile storage device (Fig. 1, #113); determining if the current content has been modified without authorization (Column 3, Lines 4-12 (validate)).

Harding et al. does not explicitly teach replacing the current content with said stored valid image of the content if the current content is determined to have been modified without authorization. However, Leavitt et al. discloses: replacing the current content with said stored valid image of the content if the current content is determined to have been modified without authorization (Fig. 3 Item 116-118). Therefore it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teachings of Leavitt et al. in conjunction with the teachings of Harding et al. for the benefit of providing alternate BIOS code blocks in case primary BIOS code blocks are invalid as taught by Leavitt et al. in Column 2, Lines 15-17.

As per **claim 17**, Harding et al. discloses: arranging a non-volatile storage device of a computer system into one or more storage regions to store CMOS BIOS data, wherein the device lacks hardware security such that some of the CMOS BIOS regions are modifiable by an application program in the system (Column 2, Lines 67-Column 3, Lines 1); generating an integrity metric corresponding to valid CMOS BIOS content stored in a first region of the non-volatile storage device (Fig. 1 #113).

Harding et al. does not explicitly teach: storing the integrity metric in another non-volatile storage device of the computer system to later determine if the content in the first region has been modified without authorization. However, Leavitt et al. discloses: storing the integrity metric in another non-volatile storage device of the computer system to later determine if the content in the first region has been modified without authorization (Fig. 3, Lines 116-118). Therefore it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teachings of Leavitt et al. in conjunction with the teachings of Harding et al. for the benefit of providing alternate BIOS code blocks in case primary BIOS code blocks are invalid as taught by Leavitt et al. in Column 2, Lines 15-17.

As per **claim 20**, Harding et al. discloses: arranging a non-volatile storage device of a computer system into one or more storage regions to store CMOS BIOS data, wherein the device lacks hardware security such that some of the CMOS BIOS regions are modifiable by an application program in the system (Column 2, Lines 67-Column 3, Lines 1); comparing current content in a first region to an earlier stored image of the content in the first region, wherein the earlier stored image is in a further non-volatile storage device (Fig. 1 #115, Column 3, Lines 4-12 and Column 3, lines 33 checksum).

Harding et al. does not explicitly teach replacing the current content stored in the first region with earlier stored image if it is determined that there was an unauthorized modification of the current content. However, Leavitt et al. discloses: replacing the current content stored in the first region with earlier stored image if it is determined that there was an unauthorized modification of the current content (Fig. 3, #116-118). Therefore it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teachings of Leavitt et al. in conjunction with the teachings of Harding et al. for the benefit of providing alternate BIOS code blocks in case primary BIOS code blocks are invalid as taught by Leavitt et al. in Column 2, Lines 15-17.

As per **claim 26**, Harding et al. discloses: reading current CMOS BIOS content stored in the non-volatile storage device (Fig. 1 #114); determining if the read current content has been modified without authorization (Column 3, Lines 23-33).

Harding et al. does not explicitly teach replacing the current content with a previously stored image of the content from a flash memory system, if the current content is determined to have been modified without authorization. However, Leavitt et al. discloses: replacing the current content with a previously stored image of the content from a flash memory system, if the current content is determined to have been modified without authorization (Fig. 3 #116-118). Therefore it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teachings of Leavitt et al. in conjunction with the teachings of Harding et al. for the benefit of providing alternate BIOS code blocks in case primary BIOS code blocks are invalid as taught by Leavitt et al. in Column 2, Lines 15-17.

As per **claims 2, 16 and 21**, rejected as applied to claims 1, 10 and 20. Furthermore, Harding et al. discloses: the processing unit is configured to process the instructions in the program store as part of a start-up procedure (Column 3, Lines 13-16).

As per **claim 3**, rejected as applied to claim 1. Furthermore, Harding et al. discloses: program store is inside said another non-volatile data storage device (Column 3, Lines 7-9).

As per **claim 4**, rejected as applied to claim 1. Furthermore, Harding et al. discloses: the processor-readable instructions in eth program store ascertain the validity of the data stored in the non-volatile storage device on a region by region basis (Column 3, Lines 23-30).

As per **claim 5**, rejected as applied to claim 1. Furthermore, Harding et al. discloses: the image of eth CMOS BIOS data is stored in a location that cannot be modified without system authorization (Column 2, Lines 61-66).

As per **claim 6**, rejected as applied to claim 5. Furthermore, Harding et al. discloses employing a system interface to perform modifications to the data stored in said another non-volatile data storage device (Column 6, Lines 66-67).

As per **claims 7 and 11**, rejected as applied to claims 1 and 10. Furthermore, Harding et al. discloses: determining if the current data in the non-volatile storage device is different than the stored image data (Harding Column 3, Lines 33-34).

As per **claim 8**, rejected as applied to claim 1. Furthermore, Harding et al. discloses: determining if an integrity metric corresponding to the current data in the non-volatile storage device is different that the same integrity metric corresponding to the stored image data (Column 3, Lines 33-34).

As per **claims 12, 27 and 28**, rejected as applied to claims 10 and 26. Furthermore, Leavitt et al. discloses: comparing a previously stored checksum, corresponding to the valid image of the content, and the checksum corresponding to the current content (Fig. 3 #144 and 142). Therefore it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teachings of Leavitt et al. in conjunction with the teachings of Harding et al. for the benefit of providing alternate BIOS code blocks in case primary BIOS code blocks are invalid as taught by Leavitt et al. in Column 2, Lines 15-17.

As per **claim 15**, rejected as applied claims 10. Furthermore, Harding et al. discloses: storing a valid image of the current content for later use (Column 5, Lines 5-16).

As per **claim 18**, rejected as applied to claim 17. Furthermore, Leavitt et al. discloses: comparing a previously stored integrity metric, corresponding to an earlier version of the content stored in the first region, to a newly calculated integrity metric corresponding to the current content stored in the first region to determine if an unauthorized modification has occurred (Fig. 3 #142). Therefore it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teachings of Leavitt et al. in conjunction with the teachings of Harding et al. for the benefit of providing alternate BIOS code blocks in case primary BIOS code blocks are invalid as taught by Leavitt et al. in Column 2, Lines 15-17.

As per **claim 19**, rejected as applied to claim 17. Furthermore, Leavitt et al. discloses: replacing the first region with an earlier version of the content therein if it is determined that there was an unauthorized modification (Fig.3 #118).

As per **claim 22**, rejected as applied to claim 20. Furthermore, Harding et al. discloses: the non-volatile storage device is arranged into one of more logical regions, each region having one or more bytes (Fig. 1 #112, 113, 114).

5. **Claims 13, 14, 29 and 30** are rejected under 35 U.S.C. 103(a) as being unpatentable over Harding et al. (U.S. Patent No. 6,651,188) in view of Leavitt et al. (U.S. Patent No. 5,918,014) in further view of Huh et al. (U.S. Patent No. 6,584,559).

As per **claims 13 and 29**, rejected as applied to claims 10 and 26. The combined references Harding et al. and Leavitt et al. substantially teach reading current CMOS BIOS content stored in a non-volatile storage device of a system, wherein the device lacks hardware security such that the CMOS BIOS content is modifiable by an application program in the system; reading from a valid image of the CMOS BIOS content, that is stored in a further non-volatile storage device; determining if the current content has been modified without authorization; and replacing the current content with said stored valid image of the content if the current content is determined to have been modified without authorization.

The combined teachings of Harding and Leavitt do not explicitly teach: comparing a previously stored cyclic redundancy check value, corresponding to the valid image of the content, and the cyclic redundancy check value corresponding to the current content. However, Huh et al. discloses: comparing a previously stored cyclic redundancy check value, corresponding to the valid image of the content, and the cyclic redundancy check value corresponding to the current content (Column 2, Lines 41-45). Therefore it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teachings of Huh et al. in conjunction with the combined teachings of Harding and Leavitt for the benefit of validating the firmware (Column 1, Lines 63-66).

As per **claims 14 and 30**, rejected as applied to claims 10 and 26. The combined references Harding et al. and Leavitt et al. substantially teach reading current CMOS BIOS content stored in a non-volatile storage device of a system, wherein the device lacks hardware security such that the CMOS BIOS content is modifiable by an application program in the system; reading from a valid image of the CMOS BIOS content, that is stored in a further non-volatile storage device; determining if the current content has been modified without authorization; and replacing the current content with said stored valid image of the content if the current content is determined to have been modified without authorization.

The combined teachings of Harding and Leavitt do not explicitly teach comparing a previously stored bit mask, corresponding to the valid image of the content, and a bit mask corresponding to the current content. However, Huh et al. discloses comparing a previously stored bit mask, corresponding to the valid image of the content, and a bit mask corresponding to the current content (Column 4, Lines 11-13). Therefore it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teachings of Huh et al. in conjunction with the combined teachings of Harding and Leavitt for the benefit of validating the firmware (Column 1, Lines 63-66).

6. **Claim 9** is rejected under 35 U.S.C. 103(a) as being unpatentable over Harding et al. (U.S. Patent No. 6,651,188) in view of Leavitt et al. (U.S. Patent No. 5,918,014) in further view of Gunderson (U.S. Patent No. 6,175,904).

As per **claim 9**, rejected as applied to claims 1. The combined references Harding and Leavitt substantially teach a non-volatile data storage device, configured as one or more storage regions to store one or more bytes of CMOS BIOS data, wherein the device lacks hardware security such that some of the CMOS BIOS regions are modifiable by an application program on the system; another non-volatile data storage device to store a mirror image of the CMOS BIOS data; a program to store one or more processor-readable instructions to ascertain the validity of the CMOS BIOS data stored in the non-volatile storage device; if invalid to replace the CMOS BIOS data in the non-volatile storage device with the mirror image of the data; and a processing unit coupled to the non-volatile storage device and program store, to read and process the one or more instructions in the program store.

The combined teachings of Harding and Leavitt do not explicitly teach generating a copy the current data in the non-volatile storage device if an authorized application modifies the current data; and storing the copy as a valid image of the current data. However, Gunderson discloses: generating a copy the current data in the non-volatile storage device if an authorized application modifies the current data; and storing the copy as a valid image of the current data (Fig. 4 #31-34). Therefore it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teachings of Gunderson in conjunction with the combined teachings of Harding and Leavitt for the benefit of backing up the data that has been changed (Fig. 4 #31).

Conclusion

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Saoussen Besrour whose telephone number is 571-272-6547. The examiner can normally be reached on M-F 8:30am to 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

SB
September 17, 2006

CHRISTOPHER REVAK
PRIMARY EXAMINER
9/18/06